ПОВЫШЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ С ПОМОЩЬЮ СКАНЕРА УЯЗВИМОСТЕЙ

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Михейчик А.Д.

Хацкевич О.А. – к.т.н., доцент

В работе рассматриваются сертифицированные сканеры уязвимостей в Республике Беларусь, с помощью которых можно осуществить повышение информационной безопасности в корпоративных сетях . Показываются основные сходства и различия между представленными сканерами, а также практическое применение одного из них.

В мае 2017 года произошла одна из самых серьезных хакерских атак, которая заразила 500 тысяч компьютеров под управлением операционной системой Microsoft Windows в 150 странах мира. Речь идет о программе-вымогателе WannaCry. Данная программа осуществляет сканирование в Интернете для нахождения открытого 445 порта (протокол SMBv1, служащий для удаленного доступа к сетевым ресурсам). После нахождения открытого 445 порта на компьютере, программа эксплуатирует на нем уязвимость EternalBlue, и в случае успеха устанавливает бэкдор DoublePulsar, благодаря которому загружается и запускается код WannaCry [1].

Для того чтобы обезопасить себя от таких программ-вымогателей, специалисты по информационной безопасности рекомендуют использовать лицензионное антивирусное программное обеспечение, автоматическое обновление операционной системы Windows, а также проверенные программные средства для предотвращения атак. В данной работе предложено использовать сканеры уязвимостей в качестве проверенных программных средств.

Сканеры уязвимостей предназначены для мониторинга сети, приложений и отдельных компьютеров на предмет нахождения проблем сетевой безопасности, а также для оценки и устранения найденных неполадок.

В Республике Беларусь существует два сертифицированных Оперативно-Аналитическим Центром сканера уязвимостей – Max Patrol 8 и PCS-1. Представленные сканеры имеют общие черты, такие как генерация отчетов в процессе завершения сканирования, список рекомендаций по их устранению, нахождения открытых портов, идентификация операционной системы, показатель критичности найденных уязвимостей. Также данные сканеры имеют и различия.

Главными особенностями Max Patrol 8 являются: удаленное сканирование, используя встроенные механизмы удаленного администрирования; возможность автоматического мониторинга сети; проверка web-приложений на нахождения уязвимостей; база данных обновляется высококвалифицированными специалистами из Positive Technologies [2].

Другой сканер, PCS-1, имеет следующие преимущества: проверка web-браузеров, установленных на компьютерах; организация защиты данных, передаваемых в пределах сети и от пользователя, от раскрытия и модификации; показывает не возможную уязвимость, а конкретную; обновляется ежедневно. В качестве серьезного недостатка можно выделить то, что при выполнении сканирования в корпоративной сети на нахождения уязвимостей, может замедлить работу фирмы, в которой осуществляется сканирование.

В качестве примера практического применения использовался сканер PCS-1. Сканируемая сеть представлена на рисунке 1.

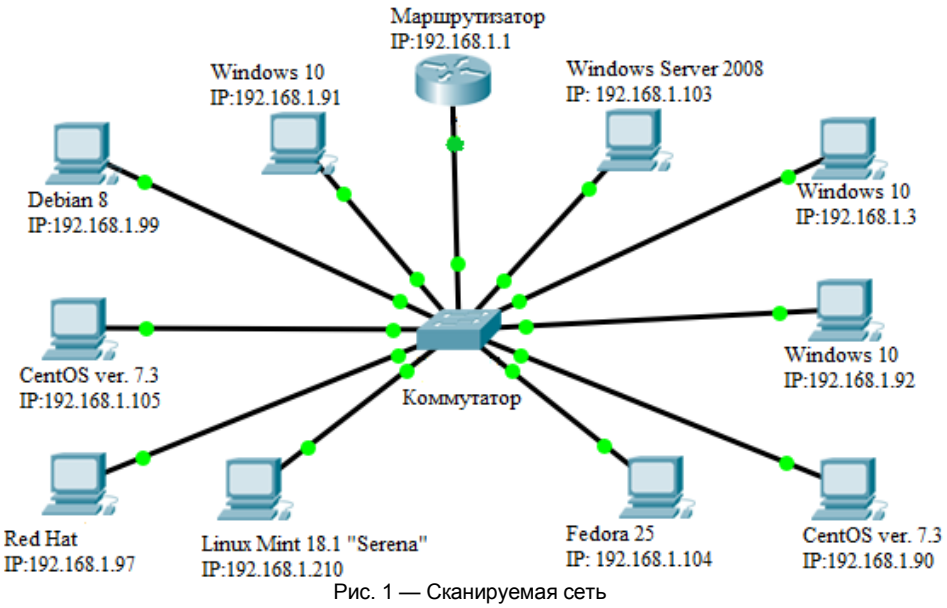

Рис. 1 — Сканируемая сеть

Сканируемая сеть, представленная на рисунке 1, представляет собой десять хостов, которые находятся в одной сети и имеют различную операционную систему. CentOS, Fedora, Linux Mint, Debian, Red Hat относятся к UNIX-подобным операционным системам. Все компьютеры подключены к коммутатору, который подключен к маршрутизатору, с помощью которого осуществляется доступ в Интернет.

При сканировании указывается либо конкретный IP-адрес, либо диапазон адресов. В данном случае указывался диапазон: 192.168.1.1 — 254.

При завершении сканирования генерируются отчеты, где указываются уязвимости, рекомендации по устранению уязвимостей, критичность уязвимости. На рисунке 2 представлена краткая общая информация: количество найденных уязвимостей, критичность уязвимостей (высокая, средняя, низкая).

Host	High	Medium	Low	Log	False Positive
192.168.1.1	2	1	0	16	0
192.168.1.103	2	10	1	31	0
192.168.1.3	0	2	1	8	0
192.168.1.91	0	2	1	8	0
192.168.1.92	0	2	0	20	0
192.168.1.210	0	1	2	18	0
192.168.1.99	0	1	0	24	0
192.168.1.105	0	0	1	6	0
192.168.1.97	0	0	1	11	0
192.168.1.104	0	0	0	4	0
192.168.1.90	0	0	0	4	0
Total: 11	4	19	7	150	0

Рис. 2 — Краткая статистика

Проанализировав рисунок 2, можно убедиться, что в сети существует 4 критических уязвимостей, 19 средних и 7 низких. С помощью сканера можно не только обнаружить, где и какие уязвимости расположены, но и, используя рекомендации, устранить их. Пример рекомендации по устранению найденной уязвимости представлен на рисунке 3.

References

CVE: CVE-2009-2526, CVE-2009-2532, CVE-2009-3103
BID: 36299
CERT: DFN-CERT-2009-1443
Other: http://www.microsoft.com/technet/security/bulletin/MS09-050.mspx

Рис.3 – Пример рекомендации по устранению найденной уязвимости

Таким образом, в данной работе показана эффективность применения сканеров уязвимостей для повышения информационной безопасности в корпоративных сетях на примере сертифицированного в Республике Беларусь сканера PCS-1.

Список использованных источников:
4. WannaCry [Электронный ресурс] – Режим доступа: https://ru.wikipedia.org/wiki/WannaCry.
5. Max Patrol 8 [Электронный ресурс] – Режим доступа: https://www.ptsecurity.com/ru-ru/products/mp8/.